ABSTRACT

A method and apparatus are described for preventing security vulnerabilities resulting from buffer overruns. According to one embodiment of the present invention, CALL is modified to place a return address on the stack, and then a random amount of space is added to the stack. This random value is placed in a known place on the stack, or kept in a non-accessible CPU register. The rest of the stack is built normally. When RET is called it finds the number of bytes added to the stack and finds the return address on the stack and returns as normal. This method allows a simple hardware solution that will not be visible to the software, yet provide a powerful deterrent to hackers looking to exploit buffer overrun vulnerabilities in software. Without any software modifications we would be able to deter a significant number of buffer overrun attacks. By affecting components lower on the environment it is possible to influence a larger set of software. For example, it is possible to affect all of the software running on the system without having to change any of the software.